EXHIBIT A

KAZEROUNI LAW GROUP, APC

245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

March 31, 2022

VIA CERTIFIED MAIL
American Financial Resources, Inc.
9 Sylvan Way
Parsippany, NJ 07054

Re: Parras, et al. v. American Financial Resources, Inc.

To Whom It May Concern:

We represent Plaintiffs Edwina and Robert Parras ("Plaintiffs") and all other similarly situated consumers in a putative class action against American Financial Resources, Inc. ("Defendant") arising out of, *inter alia*, Defendant's failure to provide reasonable security for Plaintiffs' and the proposed class members' personal information, which resulted in the unauthorized access, theft, or disclosure of this information (the "Data Breach"). To our knowledge the Data Breach occurred on between December 6-20, 2021, as specified in Defendant's "Notice of Data Breach" letter dated March 9, 2022.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiffs' Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant's conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), Plaintiffs demand that, in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiffs with an express written statement within thirty (30) days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiffs and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]

KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN: 249203)
ak@kazlg.com
Mona Amini, Esq. (SBN: 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiffs
Edwina Parras and Robert Parras
and the putative class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ALAMEDA – COMPLEX CIVIL

EDWINA PARRAS and ROBERT PARRAS, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

AMERICAN FINANCIAL RESOURCES, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*; and
3. BREACH OF CONTRACT

DEMAND FOR JURY TRIAL

KAZEROUNI LAW GROUP, APC

Plaintiffs EDWINA PARRAS AND ROBERT PARRAS ("Plaintiffs"), on behalf of themselves and the general public and all others similarly situated ("Class members"), by and through their attorneys, upon personal knowledge as to facts pertaining to themselves and on information and belief as to all other matters, brings this class action against Defendant AMERICAN FINANCIAL RESOURCES, INC. ("Defendant" or "AFR"), and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action against American Financial Resources and its related entities, subsidiaries, and agents for failing to secure and safeguard the personally identifiable information ("PII") that Defendant collected and maintained (collectively "Private Information"), and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their information had been stolen. Defendant is a residential mortgage company that serves thousands of mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and contractors across the country, with their residential financing needs.[1] For its business purposes, Defendant maintains a substantial amount of PII from its customers in its computer systems.

2. On or about March 9, 2022, Defendant announced that an unauthorized party had gained access to its computer systems and certain AFR files were accessed without authorization between December 6 to December 20, 2021 (the "Data Breach"). Defendant conducted a review of the files that were accessed in the Data Breach and on February 4, 2022 it determined files containing Plaintiffs' and other similarly situated individuals' PII, including names, Social Security numbers, and driver's license numbers were accessed in the Data Breach.

3. Although the Data Breach occurred in December 2021, placing sensitive customer information in the hands of malicious actors as a result of Defendant's failure to safeguard Plaintiffs' PII, Defendant waited months until on or around March 9, 2022 to provide notice of the Data Breach to customers. This notice was still lacking in information necessary for Plaintiffs and Class members to understand the scope and severity of the Data Breach. Due to this lapse in time between the Data Breach and Defendant's notice to affected customers, hackers may have already

[1] https://www.afrcorp.com.

been able to acquire and sell Plaintiffs' and the Class members' PII on the black market or dark web, or otherwise fraudulently misuse it for their personal gain.

4. Defendant owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected from its customers and maintained for business purposes and stored on its networks.

5. Defendant breached that duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect PII from unauthorized access and storing and retaining Plaintiffs' and Class members' personal information on inadequately protected networks.

6. The Data Breach happened because of Defendant's inadequate cybersecurity, which caused Plaintiffs' and Class members' PII to be accessed, exfiltrated, viewed, stolen and/or disclosed to unauthorized persons. This action seeks to remedy these failings. Plaintiffs bring this action on behalf of themselves individually and on behalf of all other similarly situated California residents affected by the Data Breach.

7. As set forth in the Prayer for Relief, among other things, Plaintiffs seek, for themselves and the Class, equitable relief, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

8. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiffs and Class members pursuant to Cal. Code Civ. Proc. § 382.

9. This Court has personal jurisdiction over Defendant because Defendant's regularly conducts business in California and with California consumers.

10. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because Defendant regularly conducts business in this county, and unlawful acts or omissions have occurred in this county.

PARTIES

11. At all relevant times, Plaintiffs resided in Alameda County, California. Plaintiffs are each a consumer who were customers of Defendant and provided their personal information and PII to Defendant.

12. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiffs' PII accessed, exfiltrated, viewed, stolen and/or disclosed to unauthorized persons in the Data Breach.

13. Defendant is a corporation organized under the laws of the state of New Jersey, with its principal place of business and/or headquarters located at 9 Sylvan Way, Parsippany, New Jersey 07054.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

14. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[2] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

15. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[3]

---

[2] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[3] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

16. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[4] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

17. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[5]

18. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

19. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[6] This business has created a new market for the sale and purchase of this valuable data.[7]

20. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is

---

[4] *See* Soma, *Corporate Privacy Trend, supra.*

[5] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

[6] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[7] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

21. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[9]

22. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

23. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

24. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[10]

25. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[11] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

---

[8] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#

[9] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

[10] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

[11] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

26. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[12]

27. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[13] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[14]

28. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[15] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[16] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[17]

---

[12] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

[14] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[15] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[16] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[17] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

29. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

30. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[18]

31. It is within this context that Plaintiffs and thousands of Defendant's customers must now live with the knowledge that their PII is forever in cyberspace and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Defendant's Collection of Customers' PII

32. Defendant's Privacy Statement states "American Financial Resources, Inc. (herein referred to as AFR) has been committed to your financial well-being and protecting the privacy and security of the information you share with us since our inception in 1997."[19]

33. Defendant acknowledges that it collects, stores, and transmits a substantial amount of confidential, personal, and other sensitive information from its customers for its mortgage loan origination and related services.[20] In the course of its regular business Defendant collects, at minimum, the following information:

- Social Security number and employment information including tax returns, w-2s, paystubs and related documents
- Account balances and transaction history
- Credit history and investment experience
- Social Security Number
- Current and previous home ownership experience, including physical and mailing addresses

---

[18] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

[19] *See* Defendant's Privacy Statement: https://www.afrcorp.com/privacy-statement/

[20] Defendant's "Related Services" may include, but are not limited to real estate services, insurance, escrow and other closing services, notary, appraisal, other consumer credit services, home warranty, and other services related to home purchase, home ownership, or related consumer transactions. https://www.afrcorp.com/privacy-statement/

- Letters of explanation regarding credit or employment events
- Date of birth / age
- Other information required by Defendant's investors or insurers (such as HUD)

34. With regard to its collection of Social Security numbers in particular, Defendant's Privacy Statement states:

> Social Security numbers are classified as "Confidential" information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate business "need to know" in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers collected or retained by AFR in connection with customer, employee, or other relationships.

35. The types of information Defendant collects are further detailed in its Privacy Statement (last updated February 1, 2021),[21] which for California customers, identifies the categories of personal information it may have collected about them over the past 12 months and which information is covered by the California Consumer Privacy Act ("CCPA") as follows:

- Identifiers – such as: a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.

- Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) – such as: name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, any other financial information, or medical information. Some personal information included in this category may overlap with other categories.

- Protected classification characteristics under California or federal law – such as: age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, veteran or military status, genetic information.

- Commercial information – such as: Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

---

[21] *See* Defendant's Privacy Statement: https://www.afrcorp.com/privacy-statement/

- Internet or other similar network activity – such as: Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.
- Professional or employment-related information – such as: Current or past job history or performance evaluations.
- Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)) – such as: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.
- Inferences drawn from other personal information – such as: Profile reflecting

The Data Breach

36. On or around March 9, 2022 Defendant sent official notice of the Data Breach to Plaintiffs and other customers stating, "[AFR] recently concluded an investigation into a security incident involving some of [AFR's] computer systems."

37. According to Defendant, "[AFR] conducted a comprehensive review of the files that were accessed [in the Data Breach] and, on February 4, 2022, determined that a file contained [Plaintiffs' and the Class members'] name, Social Security number, and for some individuals, driver's license number." Through its investigation "[AFR] determined that certain AFR files were accessed without authorization between December 6-20, 2021."

38. Defendant also claimed to have launched its own investigation and notified law enforcement.

39. Defendant's Notice of Data Breach letter provided little other information regarding the Data Breach itself. For instance, Defendant provided no information regarding when it learned of the Data Breach or how many people were affected by the Data Breach.

40. Following the Data Breach, Plaintiffs have experienced an amplified number of SPAM emails, have had their bank cards compromised, and have experienced fraud and financial harm in the form of unauthorized charges on Plaintiffs' account.

41. After receiving notice of the Data Breach notification letter, Plaintiffs have spent numerous hours filtering through unwanted SPAM emails which sharply increased following the Data Breach. As a result of the Data Breach, Plaintiffs have suffered an invasion and loss of their

privacy, and Plaintiffs have spent time monitoring their financial accounts, which was time that Plaintiffs otherwise would have spent performing other activities or leisurely events for the enjoyment of life rather than mitigating the impact of the Data Breach.

42. As a result of the Data Breach, Plaintiffs will continue to be at heightened risk for financial fraud, medical fraud, and/or identity theft, and the associated damages resulting from it, for years to come.

Defendant Knew or Should Have Known PII Are High Risk Targets

43. Defendant knew or should have known that PII like that at issue here, is a high-risk target for identity thieves.

44. The Identity Theft Resource Center reported that the banking/credit/financial sector had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135 data breaches exposing at least 1,709,013 million records in 2018.[22]

45. Prior to the breach there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to its subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a hacker had gained access to 100 million U.S. customer accounts and credit card applications. Similarly, in May 2019, First American Financial reported a security incident on its website that potentially exposed 885 million real estate and mortgage related documents, among others. Across industries, financial services have the second-highest cost per breached record, behind healthcare. In financial services, an average breach costs $210 per record, while a "mega breach," like Capital One's, can cost up to $388 per record.[23]

46. Anurag Kahol, CTO of Bitglass recently commented that "[g]iven that organizations in the financial services industry are entrusted with highly valuable, personally identifiable

---

[22] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[23] Samantha Ann Schwartz, *62% of breached data came from financial services in 2019*, CioDive (Dec. 23, 2019), *available at* https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/.

information (PII), they represent an attractive target for cybercriminals[.]" HelpNetSecurity reports that "[h]acking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data breaches and adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats."[24]

47. As such, Defendant was aware that PII is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiffs' and Class members' PII against cyber-security attacks that Defendant should have anticipated and guarded against.

CLASS ACTION ALLEGATIONS

48. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiffs seek to represent and intend to seek certification of a class (the "Class") defined as:

All California residents whose PII was subjected to the Data Breach.

49. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

50. Certification of Plaintiffs' claims for class wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

51. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, Defendant acknowledges the Data Breach, and based on information and belief, the Class consists of tens of thousands of Defendant's customers, including Plaintiffs

---

[24] HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), *available at* https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/.

and the Class members. Plaintiffs therefore believes that the Class is so numerous that joinder of all members is impractical.

52. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

53. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected, stored, and maintained from Plaintiffs and Class members;

(b) Whether Defendant breached its duty to protect the PII of Plaintiffs and each Class member; and

(c) Whether Plaintiffs and each Class member are entitled to damages and other equitable relief.

54. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are each an adequate representative of the Class in that Plaintiffs have no interests adverse to or that conflicts with the Class Plaintiffs seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

55. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the

costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

56. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

57. Plaintiffs reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

58. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[25]

59. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are

---

[25] CALIFORNIA CONSUMER PRIVACY ACT (CCPA) COMPLIANCE, https://buyergenomics.com/ccpa-complience/.

appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

60. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

61. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

62. Plaintiffs and Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

63. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c) does business in and is headquartered in California; and

d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or

more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

64. The PII accessed and taken by unauthorized persons in the Data Breach is "personal information" as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and Class members' unencrypted names, Social Security numbers and/or Driver's License numbers, among other personal information.

65. Plaintiffs' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including names, Social Security numbers and/or Driver's License numbers, was wrongfully accessed and taken by unauthorized persons in the Data Breach.

66. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers by hackers and to prevent unauthorized access of Plaintiffs' and Class members' PII as a result of the Data Breach.

67. On March 31, 2022, Plaintiffs provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Ex. A. If Defendant does not cure the violation within 30 days, Plaintiffs will amend their complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

68. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs, on behalf of themselves individually and the Class, seek actual damages, equitable relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")

(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)

69. Plaintiffs re-allege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

70. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the UCL.

71. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq.*) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiffs and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

72. Defendant also violated the UCL by failing to timely notify Plaintiffs and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiffs and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

73. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful

conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

74. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading, and likely to deceive the consuming public in violation of the UCL.

75. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

76. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

//

//

//

THIRD CAUSE OF ACTION

Breach of Contract

77. Plaintiffs reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

78. Plaintiffs and Class members entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

79. Plaintiffs and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their purchases of Defendant's products and services.

80. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was exposed as part of the Data Breach.

81. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves individually as well as all members of the Class respectfully request that (i) this action be certified as a class action, (ii) Plaintiffs each be designated a representative of the Class, (iii) Plaintiffs' counsel be appointed as counsel for the Class. Plaintiffs, on behalf of themselves and members of the Class further request that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) equitable relief, including restitution;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit; and

(vii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all issues so triable.

Dated: March 31, 2022

KAZEROUNI LAW GROUP, APC

By: _____

ABBAS KAZEROUNIAN, ESQ.
MONA AMINI, ESQ.

Attorneys for Plaintiffs

KAZEROUNI LAW GROUP, APC

EXHIBIT B

SUM-100

SUMMONS
(CITACION JUDICIAL)

NOTICE TO DEFENDANT:
(AVISO AL DEMANDADO):
AMERICAN FINANCIAL RESOURCES, INC.

YOU ARE BEING SUED BY PLAINTIFF:
(LO ESTÁ DEMANDANDO EL DEMANDANTE):
EDWINA PARRAS and ROBERT PARRAS, individually and on behalf of all others similarly situated

ELECTRONICALLY FILED
Superior Court of California
County of Alameda
04/01/2022
Chad Finke, Executive Officer / Clerk of the Court
By: C. Clark Deputy

NOTICE! You have been sued. The court may decide against you without your being heard unless you respond within 30 days. Read the information below.

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the plaintiff. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center (*www.courtinfo.ca.gov/selfhelp*), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site (*www.lawhelpcalifornia.org*), the California Courts Online Self-Help Center (*www.courtinfo.ca.gov/selfhelp*), or by contacting your local court or county bar association. **NOTE:** The court has a statutory lien for waived fees and costs on any settlement or arbitration award of $10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case.

¡AVISO! *Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.*

*Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al demandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California (*www.sucorte.ca.gov*), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.*

*Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services, (*www.lawhelpcalifornia.org*), en el Centro de Ayuda de las Cortes de California, (*www.sucorte.ca.gov*) o poniéndose en contacto con la corte o el colegio de abogados locales. AVISO: Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de $10,000 ó más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.*

The name and address of the court is:
(El nombre y dirección de la corte es):
Superior Court of California for the County of Alameda
1225 Falcon Street, Oakland, CA 94612

CASE NUMBER:
(Número del Caso):
22CV009276

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is:
(El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):
Abbas Kazerounian & Mona Amini - Kazerouni Law Group, APC, 245 Fischer Ave., Unit D1, Costa Mesa, California 92626 Tel: 800-400-6808

DATE: 04/01/2022 *(Fecha)*
Chad Finke, Executive Officer / Clerk of the Court
Clerk, by *(Secretario)* C. Clark , Deputy *(Adjunto)*

(For proof of service of this summons, use Proof of Service of Summons *(form POS-010).)*
(Para prueba de entrega de esta citatión use el formulario Proof of Service of Summons, *(POS-010)).*

[SEAL]

NOTICE TO THE PERSON SERVED: You are served
1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of *(specify):*
3. ☐ on behalf of *(specify):*

under: ☐ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)
☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)
☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)
☐ other *(specify):*

4. ☐ by personal delivery on *(date)*:

EXHIBIT C

KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN: 249203)
ak@kazlg.com
Mona Amini, Esq. (SBN: 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiffs
Edwina Parras and Robert Parras
and the putative class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ALAMEDA – COMPLEX CIVIL

EDWINA PARRAS and ROBERT PARRAS, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

AMERICAN FINANCIAL RESOURCES, INC.,

Defendant.

Case No. 22CV009276

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY ACT OF 2018, CAL. CIV. CODE §§ 1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *et. seq.*; and
3. BREACH OF CONTRACT

DEMAND FOR JURY TRIAL

Plaintiffs EDWINA PARRAS AND ROBERT PARRAS ("Plaintiffs"), on behalf of themselves and the general public and all others similarly situated ("Class members"), by and through their attorneys, upon personal knowledge as to facts pertaining to themselves and on information and belief as to all other matters, brings this class action against Defendant AMERICAN FINANCIAL RESOURCES, INC. ("Defendant" or "AFR"), and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action against American Financial Resources and its related entities, subsidiaries, and agents for failing to secure and safeguard the personally identifiable information ("PII") that Defendant collected and maintained (collectively "Private Information"), and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their information had been stolen. Defendant is a residential mortgage company that serves thousands of mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and contractors across the country, with their residential financing needs.[1] For its business purposes, Defendant maintains a substantial amount of PII from its customers in its computer systems.

2. On or about March 9, 2022, Defendant announced that an unauthorized party had gained access to its computer systems and certain AFR files were accessed without authorization between December 6 to December 20, 2021 (the "Data Breach"). Defendant conducted a review of the files that were accessed in the Data Breach and on February 4, 2022 it determined files containing Plaintiffs' and other similarly situated individuals' PII, including names, Social Security numbers, and driver's license numbers were accessed in the Data Breach.

3. Although the Data Breach occurred in December 2021, placing sensitive customer information in the hands of malicious actors as a result of Defendant's failure to safeguard Plaintiffs' PII, Defendant waited months until on or around March 9, 2022 to provide notice of the Data Breach to customers. This notice was still lacking in information necessary for Plaintiffs and Class members to understand the scope and severity of the Data Breach. Due to this lapse in time between the Data Breach and Defendant's notice to affected customers, hackers may have already

[1] https://www.afrcorp.com.

been able to acquire and sell Plaintiffs' and the Class members' PII on the black market or dark web, or otherwise fraudulently misuse it for their personal gain.

4. Defendant owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected from its customers and maintained for business purposes and stored on its networks.

5. Defendant breached that duty by, *inter alia*, failing to implement and maintain reasonable security procedures and practices to protect PII from unauthorized access and storing and retaining Plaintiffs' and Class members' personal information on inadequately protected networks.

6. The Data Breach happened because of Defendant's inadequate cybersecurity, which caused Plaintiffs' and Class members' PII to be accessed, exfiltrated, viewed, stolen and/or disclosed to unauthorized persons. This action seeks to remedy these failings. Plaintiffs bring this action on behalf of themselves individually and on behalf of all other similarly situated California residents affected by the Data Breach.

7. As set forth in the Prayer for Relief, among other things, Plaintiffs seek, for themselves and the Class, equitable relief, including public injunctive relief, and actual damages.

VENUE AND JURISDICTION

8. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiffs and Class members pursuant to Cal. Code Civ. Proc. § 382.

9. This Court has personal jurisdiction over Defendant because Defendant's regularly conducts business in California and with California consumers.

10. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because Defendant regularly conducts business in this county, and unlawful acts or omissions have occurred in this county.

PARTIES

11. At all relevant times, Plaintiffs resided in Alameda County, California. Plaintiffs are each a consumer who were customers of Defendant and provided their personal information and PII to Defendant.

12. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiffs' PII accessed, exfiltrated, viewed, stolen and/or disclosed to unauthorized persons in the Data Breach.

13. Defendant is a corporation organized under the laws of the state of New Jersey, with its principal place of business and/or headquarters located at 9 Sylvan Way, Parsippany, New Jersey 07054.

FACTUAL ALLEGATIONS

PII Is a Valuable Property Right that Must Be Protected

14. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.[2] California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

15. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[3]

---

[2] *See* John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[3] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

16. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[4] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

17. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[5]

18. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

19. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[6] This business has created a new market for the sale and purchase of this valuable data.[7]

20. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is

---

[4] *See* Soma, *Corporate Privacy Trend, supra*.

[5] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

[6] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[7] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

21. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[9]

22. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

23. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

24. Theft or breach of PII is serious. The California Attorney General recognizes that "[f]oundational" to every Californian's constitutional right to privacy is "information security: if companies collect consumers' personal data, they have a duty to secure it. An organization cannot protect people's privacy without being able to secure their data from unauthorized access."[10]

25. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[11] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

---

[8] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#

[9] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

[10] California Data Breach Report, Kamala D. Harris, Attorney General, California Department of Justice, February 2016.

[11] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

26. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[12]

27. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[13] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[14]

28. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[15] Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[16] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[17]

---

[12] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[14] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[15] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

[16] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[17] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

29. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

30. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[18]

31. It is within this context that Plaintiffs and thousands of Defendant's customers must now live with the knowledge that their PII is forever in cyberspace and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Defendant's Collection of Customers' PII

32. Defendant's Privacy Statement states "American Financial Resources, Inc. (herein referred to as AFR) has been committed to your financial well-being and protecting the privacy and security of the information you share with us since our inception in 1997."[19]

33. Defendant acknowledges that it collects, stores, and transmits a substantial amount of confidential, personal, and other sensitive information from its customers for its mortgage loan origination and related services.[20] In the course of its regular business Defendant collects, at minimum, the following information:

- Social Security number and employment information including tax returns, w-2s, paystubs and related documents
- Account balances and transaction history
- Credit history and investment experience
- Social Security Number
- Current and previous home ownership experience, including physical and mailing addresses

---

[18] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

[19] *See* Defendant's Privacy Statement: https://www.afrcorp.com/privacy-statement/

[20] Defendant's "Related Services" may include, but are not limited to real estate services, insurance, escrow and other closing services, notary, appraisal, other consumer credit services, home warranty, and other services related to home purchase, home ownership, or related consumer transactions. https://www.afrcorp.com/privacy-statement/

- Letters of explanation regarding credit or employment events
- Date of birth / age
- Other information required by Defendant's investors or insurers (such as HUD)

34. With regard to its collection of Social Security numbers in particular, Defendant's Privacy Statement states:

> Social Security numbers are classified as "Confidential" information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate business "need to know" in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers collected or retained by AFR in connection with customer, employee, or other relationships.

35. The types of information Defendant collects are further detailed in its Privacy Statement (last updated February 1, 2021),[21] which for California customers, identifies the categories of personal information it may have collected about them over the past 12 months and which information is covered by the California Consumer Privacy Act ("CCPA") as follows:

- Identifiers – such as: a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.

- Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) – such as: name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, any other financial information, or medical information. Some personal information included in this category may overlap with other categories.

- Protected classification characteristics under California or federal law – such as: age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, veteran or military status, genetic information.

- Commercial information – such as: Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

[21] *See* Defendant's Privacy Statement: https://www.afrcorp.com/privacy-statement/

- Internet or other similar network activity – such as: Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.

- Professional or employment-related information – such as: Current or past job history or performance evaluations.

- Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)) – such as: Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.

- Inferences drawn from other personal information – such as: Profile reflecting

The Data Breach

36. On or around March 9, 2022 Defendant sent official notice of the Data Breach to Plaintiffs and other customers stating, "[AFR] recently concluded an investigation into a security incident involving some of [AFR's] computer systems."

37. According to Defendant, "[AFR] conducted a comprehensive review of the files that were accessed [in the Data Breach] and, on February 4, 2022, determined that a file contained [Plaintiffs' and the Class members'] name, Social Security number, and for some individuals, driver's license number." Through its investigation "[AFR] determined that certain AFR files were accessed without authorization between December 6-20, 2021."

38. Defendant also claimed to have launched its own investigation and notified law enforcement.

39. Defendant's Notice of Data Breach letter provided little other information regarding the Data Breach itself. For instance, Defendant provided no information regarding when it learned of the Data Breach or how many people were affected by the Data Breach.

40. Following the Data Breach, Plaintiffs have experienced an amplified number of SPAM emails, have had their bank cards compromised, and have experienced fraud and financial harm in the form of unauthorized charges on Plaintiffs' account.

41. After receiving notice of the Data Breach notification letter, Plaintiffs have spent numerous hours filtering through unwanted SPAM emails which sharply increased following the Data Breach. As a result of the Data Breach, Plaintiffs have suffered an invasion and loss of their

privacy, and Plaintiffs have spent time monitoring their financial accounts, which was time that Plaintiffs otherwise would have spent performing other activities or leisurely events for the enjoyment of life rather than mitigating the impact of the Data Breach.

42. As a result of the Data Breach, Plaintiffs will continue to be at heightened risk for financial fraud, medical fraud, and/or identity theft, and the associated damages resulting from it, for years to come.

Defendant Knew or Should Have Known PII Are High Risk Targets

43. Defendant knew or should have known that PII like that at issue here, is a high-risk target for identity thieves.

44. The Identity Theft Resource Center reported that the banking/credit/financial sector had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135 data breaches exposing at least 1,709,013 million records in 2018.[22]

45. Prior to the breach there were many reports of high-profile data breaches that should have put a company like Defendant on high alert and forced it to closely examine its own security procedures, as well as those of third parties with which it did business and gave access to its subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a hacker had gained access to 100 million U.S. customer accounts and credit card applications. Similarly, in May 2019, First American Financial reported a security incident on its website that potentially exposed 885 million real estate and mortgage related documents, among others. Across industries, financial services have the second-highest cost per breached record, behind healthcare. In financial services, an average breach costs $210 per record, while a "mega breach," like Capital One's, can cost up to $388 per record.[23]

46. Anurag Kahol, CTO of Bitglass recently commented that "[g]iven that organizations in the financial services industry are entrusted with highly valuable, personally identifiable

---

[22] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[23] Samantha Ann Schwartz, *62% of breached data came from financial services in 2019*, CioDive (Dec. 23, 2019), *available at* https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/.

information (PII), they represent an attractive target for cybercriminals[.]" HelpNetSecurity reports that "[h]acking and malware are leading the charge against financial services and the costs associated with breaches are growing. Financial services organizations must get a handle on data breaches and adopt a proactive security strategy if they are to properly protect data from an evolving variety of threats."[24]

47. As such, Defendant was aware that PII is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiffs' and Class members' PII against cyber-security attacks that Defendant should have anticipated and guarded against.

CLASS ACTION ALLEGATIONS

48. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiffs seek to represent and intend to seek certification of a class (the "Class") defined as:

All California residents whose PII was subjected to the Data Breach.

49. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

50. Certification of Plaintiffs' claims for class wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

51. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, Defendant acknowledges the Data Breach, and based on information and belief, the Class consists of tens of thousands of Defendant's customers, including Plaintiffs

[24] HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), *available at* https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/.

and the Class members. Plaintiffs therefore believes that the Class is so numerous that joinder of all members is impractical.

52. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

53. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

(a) Whether Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII it collected, stored, and maintained from Plaintiffs and Class members;

(b) Whether Defendant breached its duty to protect the PII of Plaintiffs and each Class member; and

(c) Whether Plaintiffs and each Class member are entitled to damages and other equitable relief.

54. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are each an adequate representative of the Class in that Plaintiffs have no interests adverse to or that conflicts with the Class Plaintiffs seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

55. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the

costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

56. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code §§ 1798.100, *et seq.*

57. Plaintiffs reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

58. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[25]

59. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are

[25] CALIFORNIA CONSUMER PRIVACY ACT (CCPA) COMPLIANCE, https://buyergenomics.com/ccpa-complience/.

appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

60. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." 1798.81.5(c).

61. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

62. Plaintiffs and Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

63. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a) is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b) "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c) does business in and is headquartered in California; and

d) has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or

more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

64. The PII accessed and taken by unauthorized persons in the Data Breach is "personal information" as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and Class members' unencrypted names, Social Security numbers and/or Driver's License numbers, among other personal information.

65. Plaintiffs' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including names, Social Security numbers and/or Driver's License numbers, was wrongfully accessed and taken by unauthorized persons in the Data Breach.

66. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers by hackers and to prevent unauthorized access of Plaintiffs' and Class members' PII as a result of the Data Breach.

67. On March 31, 2022, Plaintiffs provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Ex. A. If Defendant does not cure the violation within 30 days, Plaintiffs will amend their complaint to pursue statutory damages as permitted by Civil Code § 1798.150(a)(1)(A).

68. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs, on behalf of themselves individually and the Class, seek actual damages, equitable relief, including public injunctive relief, and declaratory relief, and any other relief as deemed appropriate by the Court.

SECOND CAUSE OF ACTION

Violation of the California Unfair Competition Law ("UCL")

(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)

69. Plaintiffs re-allege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

70. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning, and in violation of, the UCL.

71. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiffs and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

72. Defendant also violated the UCL by failing to timely notify Plaintiffs and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiffs and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

73. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful

conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

74. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading, and likely to deceive the consuming public in violation of the UCL.

75. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

76. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

//

//

//

THIRD CAUSE OF ACTION

Breach of Contract

77. Plaintiffs reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

78. Plaintiffs and Class members entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

79. Plaintiffs and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their purchases of Defendant's products and services.

80. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was exposed as part of the Data Breach.

81. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves individually as well as all members of the Class respectfully request that (i) this action be certified as a class action, (ii) Plaintiffs each be designated a representative of the Class, (iii) Plaintiffs' counsel be appointed as counsel for the Class. Plaintiffs, on behalf of themselves and members of the Class further request that upon final trial or hearing, judgment be awarded against Defendant for:

(i) actual and punitive damages to be determined by the trier of fact;

(ii) equitable relief, including restitution;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iv) appropriate injunctive relief;

(v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;

(vi) costs of suit; and

(vii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all issues so triable.

Dated: March 31, 2022

KAZEROUNI LAW GROUP, APC

By: _____

ABBAS KAZEROUNIAN, ESQ.
MONA AMINI, ESQ.

Attorneys for Plaintiffs

EXHIBIT A

KAZEROUNI LAW GROUP, APC

245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

March 31, 2022

VIA CERTIFIED MAIL
American Financial Resources, Inc.
9 Sylvan Way
Parsippany, NJ 07054

Re: Parras, et al. v. American Financial Resources, Inc.

To Whom It May Concern:

We represent Plaintiffs Edwina and Robert Parras ("Plaintiffs") and all other similarly situated consumers in a putative class action against American Financial Resources, Inc. ("Defendant") arising out of, *inter alia*, Defendant's failure to provide reasonable security for Plaintiffs' and the proposed class members' personal information, which resulted in the unauthorized access, theft, or disclosure of this information (the "Data Breach"). To our knowledge the Data Breach occurred on between December 6-20, 2021, as specified in Defendant's "Notice of Data Breach" letter dated March 9, 2022.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiffs' Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant's conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), Plaintiffs demand that, in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiffs with an express written statement within thirty (30) days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiffs and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]

EXHIBIT D

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address):
Abbas Kazerounian (249203); Mona Amini (296829)
KAZEROUNI LAW GROUP, APC
245 Fischer Ave., Unit D1, Costa Mesa, CA 92626

TELEPHONE NO.: (800) 400-6808 FAX NO. (Optional): (800) 520-5523
ATTORNEY FOR (Name): Edwina Parras and Robert Parras

FOR COURT USE ONLY

ELECTRONICALLY FILED
Superior Court of California,
County of Alameda
04/01/2022 at 12:00:00 AM
By: Cheryl Clark, Deputy Clerk

SUPERIOR COURT OF CALIFORNIA, COUNTY OF ALAMEDA
STREET ADDRESS: 1225 Fallon Street
MAILING ADDRESS:
CITY AND ZIP CODE: Oakland, CA 94612
BRANCH NAME: Oakland - Rene C. Davidson Courthouse

CASE NAME:
Parras, et al. v. American Financial Resources, Inc.

CASE NUMBER:
22CV009276

JUDGE:
DEPT.:

CIVIL CASE COVER SHEET

[x] **Unlimited** (Amount demanded exceeds $25,000)
[ ] **Limited** (Amount demanded is $25,000)

Complex Case Designation

[ ] Counter [ ] Joinder
Filed with first appearance by defendant (Cal. Rules of Court, rule 3.402)

Items 1–6 below must be completed (see instructions on page 2).

1. Check **one** box below for the case type that best describes this case:

Auto Tort
- [ ] Auto (22)
- [ ] Uninsured motorist (46)

Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort
- [ ] Asbestos (04)
- [ ] Product liability (24)
- [ ] Medical malpractice (45)
- [ ] Other PI/PD/WD (23)

Non-PI/PD/WD (Other) Tort
- [ ] Business tort/unfair business practice (07)
- [ ] Civil rights (08)
- [ ] Defamation (13)
- [ ] Fraud (16)
- [ ] Intellectual property (19)
- [ ] Professional negligence (25)
- [x] Other non-PI/PD/WD tort (35)

Employment
- [ ] Wrongful termination (36)
- [ ] Other employment (15)

Contract
- [ ] Breach of contract/warranty (06)
- [ ] Rule 3.740 collections (09)
- [ ] Other collections (09)
- [ ] Insurance coverage (18)
- [ ] Other contract (37)

Real Property
- [ ] Eminent domain/Inverse condemnation (14)
- [ ] Wrongful eviction (33)
- [ ] Other real property (26)

Unlawful Detainer
- [ ] Commercial (31)
- [ ] Residential (32)
- [ ] Drugs (38)

Judicial Review
- [ ] Asset forfeiture (05)
- [ ] Petition re: arbitration award (11)
- [ ] Writ of mandate (02)
- [ ] Other judicial review (39)

Provisionally Complex Civil Litigation (Cal. Rules of Court, rules 3.400–3.403)
- [ ] Antitrust/Trade regulation (03)
- [ ] Construction defect (10)
- [ ] Mass tort (40)
- [ ] Securities litigation (28)
- [ ] Environmental/Toxic tort (30)
- [ ] Insurance coverage claims arising from the above listed provisionally complex case types (41)

Enforcement of Judgment
- [ ] Enforcement of judgment (20)

Miscellaneous Civil Complaint
- [ ] RICO (27)
- [ ] Other complaint *(not specified above)* (42)

Miscellaneous Civil Petition
- [ ] Partnership and corporate governance (21)
- [ ] Other petition *(not specified above)* (43)

2. This case [x] is [ ] is not complex under rule 3.400 of the California Rules of Court. If the case is complex, mark the factors requiring exceptional judicial management:
   a. [ ] Large number of separately represented parties
   b. [x] Extensive motion practice raising difficult or novel issues that will be time-consuming to resolve
   c. [x] Substantial amount of documentary evidence
   d. [x] Large number of witnesses
   e. [ ] Coordination with related actions pending in one or more courts in other counties, states, or countries, or in a federal court
   f. [ ] Substantial postjudgment judicial supervision
3. Remedies sought *(check all that apply):* a. [x] monetary b. [x] nonmonetary; declaratory or injunctive relief c. [x] punitive
4. Number of causes of action *(specify):*
5. This case [x] is [ ] is not a class action suit.
6. If there are any known related cases, file and serve a notice of related case. *(You may use form CM-015.)*

Date: March 31, 2022
Abbas Kazerounian
(TYPE OR PRINT NAME)

(SIGNATURE OF PARTY OR ATTORNEY FOR PARTY)

NOTICE

- Plaintiff must file this cover sheet with the first paper filed in the action or proceeding (except small claims cases or cases filed under the Probate Code, Family Code, or Welfare and Institutions Code). (Cal. Rules of Court, rule 3.220.) Failure to file may result in sanctions.
- File this cover sheet in addition to any cover sheet required by local court rule.
- If this case is complex under rule 3.400 et seq. of the California Rules of Court, you must serve a copy of this cover sheet on all other parties to the action or proceeding.
- Unless this is a collections case under rule 3.740 or a complex case, this cover sheet will be used for statistical purposes only.

INSTRUCTIONS ON HOW TO COMPLETE THE COVER SHEET

CM-010

To Plaintiffs and Others Filing First Papers. If you are filing a first paper (for example, a complaint) in a civil case, you **must** complete and file, along with your first paper, the Civil Case Cover Sheet contained on page 1. This information will be used to compile statistics about the types and numbers of cases filed. You must complete items 1 through 6 on the sheet. In item 1, you must check **one** box for the case type that best describes the case. If the case fits both a general and a more specific type of case listed in item 1, check the more specific one. If the case has multiple causes of action, check the box that best indicates the **primary** cause of action. To assist you in completing the sheet, examples of the cases that belong under each case type in item 1 are provided below. A cover sheet must be filed only with your initial paper. Failure to file a cover sheet with the first paper filed in a civil case may subject a party, its counsel, or both to sanctions under rules 2.30 and 3.220 of the California Rules of Court.

To Parties in Rule 3.740 Collections Cases. A "collections case" under rule 3.740 is defined as an action for recovery of money owed in a sum stated to be certain that is not more than $25,000, exclusive of interest and attorney's fees, arising from a transaction in which property, services, or money was acquired on credit. A collections case does not include an action seeking the following: (1) tort damages, (2) punitive damages, (3) recovery of real property, (4) recovery of personal property, or (5) a prejudgment writ of attachment. The identification of a case as a rule 3.740 collections case on this form means that it will be exempt from the general time-for-service requirements and case management rules, unless a defendant files a responsive pleading. A rule 3.740 collections case will be subject to the requirements for service and obtaining a judgment in rule 3.740.

To Parties in Complex Cases. In complex cases only, parties must also use the Civil Case Cover Sheet to designate whether the case is complex. If a plaintiff believes the case is complex under rule 3.400 of the California Rules of Court, this must be indicated by completing the appropriate boxes in items 1 and 2. If a plaintiff designates a case as complex, the cover sheet must be served with the complaint on all parties to the action. A defendant may file and serve no later than the time of its first appearance a joinder in the plaintiff's designation, a counter-designation that the case is not complex, or, if the plaintiff has made no designation, a designation that the case is complex.

CASE TYPES AND EXAMPLES

Auto Tort
- Auto (22)–Personal Injury/Property Damage/Wrongful Death
- Uninsured Motorist (46) *(if the case involves an uninsured motorist claim subject to arbitration, check this item instead of Auto)*

Other PI/PD/WD (Personal Injury/ Property Damage/Wrongful Death) Tort
- Asbestos (04)
  - Asbestos Property Damage
  - Asbestos Personal Injury/ Wrongful Death
- Product Liability *(not asbestos or toxic/environmental)* (24)
- Medical Malpractice (45)
  - Medical Malpractice–Physicians & Surgeons
- Other Professional Health Care Malpractice
- Other PI/PD/WD (23)
  - Premises Liability (e.g., slip and fall)
  - Intentional Bodily Injury/PD/WD (e.g., assault, vandalism)
  - Intentional Infliction of Emotional Distress
  - Negligent Infliction of Emotional Distress
  - Other PI/PD/WD

Non-PI/PD/WD (Other) Tort
- Business Tort/Unfair Business Practice (07)
- Civil Rights (e.g., discrimination, false arrest) *(not civil harassment)* (08)
- Defamation (e.g., slander, libel) (13)
- Fraud (16)
- Intellectual Property (19)
- Professional Negligence (25)
  - Legal Malpractice
  - Other Professional Malpractice *(not medical or legal)*
- Other Non-PI/PD/WD Tort (35)

Employment
- Wrongful Termination (36)
- Other Employment (15)

Contract
- Breach of Contract/Warranty (06)
  - Breach of Rental/Lease Contract *(not unlawful detainer or wrongful eviction)*
  - Contract/Warranty Breach–Seller Plaintiff *(not fraud or negligence)*
  - Negligent Breach of Contract/ Warranty
  - Other Breach of Contract/Warranty
- Collections (e.g., money owed, open book accounts) (09)
  - Collection Case–Seller Plaintiff
  - Other Promissory Note/Collections Case
- Insurance Coverage *(not provisionally complex)* (18)
  - Auto Subrogation
  - Other Coverage
- Other Contract (37)
  - Contractual Fraud
  - Other Contract Dispute

Real Property
- Eminent Domain/Inverse Condemnation (14)
- Wrongful Eviction (33)
- Other Real Property (e.g., quiet title) (26)
  - Writ of Possession of Real Property
  - Mortgage Foreclosure
  - Quiet Title
  - Other Real Property *(not eminent domain, landlord/tenant, or foreclosure)*

Unlawful Detainer
- Commercial (31)
- Residential (32)
- Drugs (38) *(if the case involves illegal drugs, check this item; otherwise, report as Commercial or Residential)*

Judicial Review
- Asset Forfeiture (05)
- Petition Re: Arbitration Award (11)
- Writ of Mandate (02)
  - Writ–Administrative Mandamus
  - Writ–Mandamus on Limited Court Case Matter
  - Writ–Other Limited Court Case Review
- Other Judicial Review (39)
  - Review of Health Officer Order
  - Notice of Appeal–Labor Commissioner Appeals

Provisionally Complex Civil Litigation (Cal. Rules of Court Rules 3.400–3.403)
- Antitrust/Trade Regulation (03)
- Construction Defect (10)
- Claims Involving Mass Tort (40)
- Securities Litigation (28)
- Environmental/Toxic Tort (30)
- Insurance Coverage Claims *(arising from provisionally complex case type listed above)* (41)

Enforcement of Judgment
- Enforcement of Judgment (20)
  - Abstract of Judgment (Out of County)
- Confession of Judgment *(non-domestic relations)*
- Sister State Judgment
- Administrative Agency Award *(not unpaid taxes)*
- Petition/Certification of Entry of Judgment on Unpaid Taxes
- Other Enforcement of Judgment Case

Miscellaneous Civil Complaint
- RICO (27)
- Other Complaint *(not specified above)* (42)
  - Declaratory Relief Only
  - Injunctive Relief Only *(non-harassment)*
  - Mechanics Lien
  - Other Commercial Complaint Case *(non-tort/non-complex)*
  - Other Civil Complaint *(non-tort/non-complex)*

Miscellaneous Civil Petition
- Partnership and Corporate Governance (21)
- Other Petition *(not specified above)* (43)
  - Civil Harassment
  - Workplace Violence
  - Elder/Dependent Adult Abuse
  - Election Contest
  - Petition for Name Change
  - Petition for Relief From Late Claim
  - Other Civil Petition

For your protection and privacy, please press the Clear This Form button after you have printed the form.

Print this form | Save this form | Clear this form

F. ADDENDUM TO CIVIL CASE COVER SHEET

Short Title: **Case Number:**

CIVIL CASE COVER SHEET ADDENDUM

THIS FORM IS REQUIRED IN ALL NEW UNLIMITED CIVIL CASE FILINGS IN THE SUPERIOR COURT OF CALIFORNIA, COUNTY OF ALAMEDA

[ ] Oakland, Rene C. Davidson Alameda County Courthouse (446)
[ ] Hayward Hall of Justice (447)
[ ] Pleasanton, Gale-Schenone Hall of Justice (448)

Civil Case Cover Sheet Category	Civil Case Cover Sheet Case Type	Alameda County Case Type (check only one)
Auto Tort	Auto tort (22)	[ ] 34 Auto tort (G) **Is this an uninsured motorist case? [ ] yes [ ] no**
Other PI /PD / WD Tort	Asbestos (04)	[ ] 75 Asbestos (D)
	Product liability (24)	[ ] 89 Product liability (not asbestos or toxic tort/environmental) (G)
	Medical malpractice (45)	[ ] 97 Medical malpractice (G)
	Other PI/PD/WD tort (23)	[ ] 33 Other PI/PD/WD tort (G)
Non - PI /PD / WD Tort	Bus tort / unfair bus. practice (07)	[ ] 79 Bus tort / unfair bus. practice (G)
	Civil rights (08)	[ ] 80 Civil rights (G)
	Defamation (13)	[ ] 84 Defamation (G)
	Fraud (16)	[ ] 24 Fraud (G)
	Intellectual property (19)	[ ] 87 Intellectual property (G)
	Professional negligence (25)	[ ] 59 Professional negligence - non-medical (G)
	Other non-PI/PD/WD tort (35)	[ ] 03 Other non-PI/PD/WD tort (G)
Employment	Wrongful termination (36)	[ ] 38 Wrongful termination (G)
	Other employment (15)	[ ] 85 Other employment (G)
		[ ] 53 Labor comm award confirmation
		[ ] 54 Notice of appeal - L.C.A.
Contract	Breach contract / Wrnty (06)	[ ] 04 Breach contract / Wrnty (G)
	Collections (09)	[ ] 81 Collections (G)
	Insurance coverage (18)	[ ] 86 Ins. coverage - non-complex (G)
	Other contract (37)	[ ] 98 Other contract (G)
Real Property	Eminent domain / Inv Cdm (14)	[ ] 18 Eminent domain / Inv Cdm (G)
	Wrongful eviction (33)	[ ] 17 Wrongful eviction (G)
	Other real property (26)	[ ] 36 Other real property (G)
Unlawful Detainer	Commercial (31)	[ ] 94 Unlawful Detainer - commercial **Is the deft. in possession**
	Residential (32)	[ ] 47 Unlawful Detainer - residential **of the property?**
	Drugs (38)	[ ] 21 Unlawful detainer - drugs **[ ] Yes [ ] No**
Judicial Review	Asset forfeiture (05)	[ ] 41 Asset forfeiture
	Petition re: arbitration award (11)	[ ] 62 Pet. re: arbitration award
	Writ of Mandate (02)	[ ] 49 Writ of mandate **Is this a CEQA action (Publ.Res.Code section 21000 et seq) [ ] Yes [ ] No**
	Other judicial review (39)	[ ] 64 Other judicial review
Provisionally Complex	Antitrust / Trade regulation (03)	[ ] 77 Antitrust / Trade regulation
	Construction defect (10)	[ ] 82 Construction defect
	Claims involving mass tort (40)	[ ] 78 Claims involving mass tort
	Securities litigation (28)	[ ] 91 Securities litigation
	Toxic tort / Environmental (30)	[ ] 93 Toxic tort / Environmental
	Ins covrg from cmplx case type (41)	[ ] 95 Ins covrg from complex case type
Enforcement of Judgment	Enforcement of judgment (20)	[ ] 19 Enforcement of judgment
		[ ] 08 Confession of judgment
Misc Complaint	RICO (27)	[ ] 90 RICO (G)
	Partnership / Corp. governance (21)	[ ] 88 Partnership / Corp. governance (G)
	Other complaint (42)	[ ] 68 All other complaints (G)
Misc. Civil Petition	Other petition (43)	[ ] 06 Change of name
		[ ] 69 Other petition

EXHIBIT E

SUPERIOR COURT OF CALIFORNIA COUNTY OF ALAMEDA	Reserved for Clerk's File Stamp FILED Superior Court of California County of Alameda 04/01/2022 Chad Finke, Executive Officer / Clerk of the Court By: Deputy C. Clark
COURTHOUSE ADDRESS: Rene C. Davidson Courthouse 1225 Fallon Street, Oakland, CA 94612	
PLAINTIFF: Edwina Parras et al	
DEFENDANT: American Financial Resources, Inc.	
NOTICE OF CASE MANAGEMENT CONFERENCE	CASE NUMBER: 22CV009276

TO THE PLAINTIFF(S)/ATTORNY(S) FOR PLAINTIFF(S) OF RECORD:

You are ordered to serve all named defendants and file proofs of service on those defendants with the court within 60 days of the filing of the complaint (Cal. Rules of Court, 3.110(b)).

Give notice of this conference to all other parties and file proof of service.

Your Case Management Conference has been scheduled on:

Date: 08/01/2022 Time: 8:30 AM Dept.: 21

Location: Rene C. Davidson Courthouse
Administration Building, 1221 Oak Street, Oakland, CA 94612

TO DEFENDANT(S)/ATTORNEY(S) FOR DEFENDANT(S) OF RECORD:

The setting of the Case Management Conference does not exempt the defendant from filing a responsive pleading as required by law, you must respond as stated on the summons.

TO ALL PARTIES who have appeared before the date of the conference must:

Pursuant to California Rules of Court, 3.725, a completed Case Management Statement (Judicial Council form CM-110) must be filed and served at least 15 calendar days before the Case Management Conference. The Case Management Statement may be filed jointly by all parties/attorneys of record or individually by each party/attorney of record.

Meet and confer, in person or by telephone as required by Cal. Rules of Court, rule 3.724.

Post jury fees as required by Code of Civil Procedure section 631.

If you do not follow the orders above, the court may issue an order to show cause why you should not be sanctioned under Cal. Rules of Court, rule 2.30. Sanctions may include monetary sanctions, striking pleadings or dismissal of the action.

The judge may place a Tentative Case Management Order in your case's on-line register of actions before the conference. This order may establish a discovery schedule, set a trial date or refer the case to Alternate Dispute Resolution, such as mediation or arbitration. Check the court's eCourt Public Portal for each assigned department's procedures regarding tentative case management orders at https://eportal.alameda.courts.ca.gov.

SUPERIOR COURT OF CALIFORNIA COUNTY OF ALAMEDA	Reserved for Clerk's File Stamp FILED Superior Court of California County of Alameda 04/01/2022 Chad Finke, Executive Officer / Clerk of the Court By: C. Clark Deputy
COURTHOUSE ADDRESS: Rene C. Davidson Courthouse 1225 Fallon Street, Oakland, CA 94612	
PLAINTIFF/PETITIONER: Edwina Parras et al	
DEFENDANT/RESPONDENT: American Financial Resources, Inc.	
CERTIFICATE OF MAILING	CASE NUMBER: 22CV009276

I, the below-named Executive Officer/Clerk of the above-entitled court, do hereby certify that I am not a party to the cause herein, and that on this date I served the Notice of Case Management Conference upon each party or counsel named below by placing the document for collection and mailing so as to cause it to be deposited in the United States mail at the courthouse in Oakland, California, one copy of the original filed/entered herein in a separate sealed envelope to each address as shown below with the postage thereon fully prepaid, in accordance with standard court practices.

Chad Finke, Executive Officer / Clerk of the Court

Dated: 04/04/2022

By:

C. Clark, Deputy Clerk

CERTIFICATE OF MAILING